



Notice of Allowability

Application No.

09/554,419

Examiner

Matthew B Smithers

Applicant(s)

SPRAGGS, LYNN

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--
All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to a petition filed 30 April 2004.
2. ☒ The allowed claim(s) is/are 15-47; 1-33.
3. ☒ The drawings filed on 29 June 2000 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Lynn Spraggs on September 17, 2004.

The application has been amended as follows:

IN THE CLAIMS:

15. (New) A system for using a shared key to transmit secure data between a client and a server, the system comprising:

an encrypt/decrypt engine for using the shared key to encrypt or decrypt data, the encrypt/decrypt engine being configured for delivery via a web page to a client in response to a user request and further configured to encrypt data independently of an identity of the physical client;

wherein the server includes a user private keys database configured to store the shared key, ~~[[.]] And,~~ and wherein, it is possible for the client and the server to reside on the same physical computing device, ~~[[.]] And when~~ and where the shared key is

derived from the user's authentication data, and the derived shared key is used for encrypting all data.

16. (Previously) The system of claim 15 wherein the shared key is a user's private key entered by a user into the web page.

17. (Previously) The system of claim 15 further comprising a secure data database configured to store data received from the client and, upon the completion of a processing step, to deliver the stored data in an encrypted format to the client or to another client.

18. (Previously) The system of claim 15 further comprising a secure data database configured to store data received from the client and, upon receipt of a request for the data, to deliver the stored data in an encrypted format to the client or to another client.

19. (New) The system of claim 15 wherein the shared key is transmitted between the server and the client as few as zero times and the shared key is transmitted between the server and the user as few as one time. ~~[[.]] The,~~ the key is not sent for authentication purposes, rather, the effect of the key in the encryption process is sent, [[.]] Consequently, consequently, the shared key does not need to be retransmitted once it has been established.

20. (Previously) The system of claim 15 wherein the shared key is a user's private key entered by a user.

21. (Previously) The system of claim 15 wherein the client encrypt/decrypt engine is installed on the client.

22. (New) A system for using a shared key in transmitting secure data between a client and a server, the system comprising:

an encrypt/decrypt engine for using, the shared key, in encrypting data, the encrypt/decrypt engine being configured to encrypt data independently of an identity of the client;

and a user private keys database located on the server and configured to store the shared key, the shared key being the private key of a user, ~~[[.]]~~ And when and where the shared key is derived from the user's authentication data, and the derived shared key is used for encrypting all data.

23. (New) The system of claim 22 wherein the server is configured to decrypt encrypted data received from the client using the shared key and to use a private server key, known only by the server, to re-encrypt the decrypted data.

24. (New) The system of claim 23 further comprising a secure data database configured to store the encrypted data received from the client and re-encrypted by the server and to deliver the stored data to the client or to another client; the delivered data, after the completion of a processing step, being encrypted with the shared user key or with another shared user key, ~~[[.]]~~ And when and where the shared key is derived from the user's authentication data, and the derived shared key is used for encrypting all data.

25. (New) The system of claim 23 further comprising a secure data database configured to store the encrypted data received from the client and re-encrypted by the server and to deliver the stored data to the client or to another client; the delivered data being, upon receipt of a request for the data, encrypted with the shared user key or with another

shared user key, where the shared key is derived from the user's authentication data, and the derived shared key is used for encrypting all data.

26. (Previously) The system of claim 25 wherein the request is from the user.

27. (Previously) The system of claim 25 wherein the request is from an other user.

28. (New) A system for using a shared key in transmitting secure data between a client and a server, the system comprising:

an encrypt/decrypt engine for using the shared key entered by a user to encrypt data entered by the user, the encrypt/decrypt engine being configured such that all data entered by the user and stored on the client is stored in encrypted form, and further configured to encrypt data independently of an identity of the physical client; the shared key entry being the responsibility of the user and not the client; the server including a user private keys database configured to store the shared key, the shared key being a private key of a user; and not a physical client and, when where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data.

29. (Previously) The system of claim 28, wherein the encrypt/decrypt engine uses a symmetric key encryption/decryption algorithm for encrypting and decrypting data.

30. (Previously) The system of claim 28, further including a web server engine configured for the user to securely send or receive data from the client to the server.

31. (New) A method for using a shared key in receiving secure data on a server, comprising the steps of:

delivering from a server to a client a web page including an encrypt/decrypt engine; encrypting data on the client using the encrypt/decrypt engine and a shared key entered by a user of the client, the shared key being shared between the user and the server;

delivering the encrypted data from the client to the server; ~~when~~ where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data; receiving the encrypted data at the server; decrypting the encrypted data at the server using the shared

key; and processing the decrypted data, ~~when~~ where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data.

32. (Previously) The method of claim 31, wherein the step of processing the decrypted data includes the steps of: encrypting the decrypted data with a private server key; and storing the encrypted data in a database.

33. (Previously) The method of claim 31, wherein the step of processing the decrypted data includes the steps of: re-encrypting the data with an other user's private key shared between the other user and the server; and sending the re-encrypted data to the other user.

34. (Previously) The method of claim 31, wherein the step of processing the decrypted data includes the steps of: decrypting the encrypted data with the private server key; re-encrypting the data with a second user's key shared between the second user and the server; and sending the re-encrypted data to the second user.

35. (Previously) The method of claim 31, wherein the step of processing the decrypted data includes the steps of: processing the data according to an instruction of the user; re-encrypting the processed data using the user's shared key; and sending the re-encrypted processed data to the user.

36. (Previously) The method of claim 31, wherein the step of, processing the decrypted data includes storing the decrypted data in a secure database.

37. (New) A computer-readable medium comprising program instructions for causing a computer system to use a shared key in receiving secure data at a server, by the steps of:

delivering a web page from the server to a client, the web page including an encrypt/decrypt engine and being configured to use the encrypt/decrypt engine and a shared key entered by a user of the client to encrypt data on the client; the shared key being shared between the user and the server; receiving the encrypted data at then server; decrypting the encrypted data using the shared key; and processing the decrypted data ~~and when~~ where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data.

38. (New) A computer-readable medium comprising program instructions for causing a computer system to receive secure data on a server using a shared key, by the steps of: delivering an encrypt/ decrypt engine from the server to a client, the encrypt/decrypt engine being configured to use a shared key entered by a user of the client to encrypt data on the client, the shared key being shared between the user and the server and the encryption being independent of an identity of the physical client; receiving the

Art Unit: 2137

encrypted data at the server; decrypting the encrypted data using the shared key; and processing the decrypted data, ~~when~~ where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data.

39. (Previously) The computer readable medium of claim 38, further comprising program instructions for causing the processed decrypted data to be re-encrypted using a private server key.

40. (Previously) The computer-readable medium of claim 39, further comprising program instructions for causing the processed decrypted data to be stored in a secure database.

41. (Previously) The computer-readable medium of claim 38, wherein processing the decrypted data includes the steps of: re-encrypting the data with the private server key; storing the re-encrypted data; decrypting the stored data with the private server key; encrypting the data with a second user's key shared between the second user and the server; and sending the encrypted data to the second user.

42. (Previously) The computer-readable medium of claim 38 wherein processing the decrypted data includes the steps of: processing the data according to an instruction of the user; encrypting the processed data using a shared key; and sending the encrypted processed data to the user or to another user.

43. (New) A method of using a shared key in transmitting secure data between a client and a server using a shared key, comprising the steps of: encrypting data using the shared key with an encrypt/decrypt engine configured to encrypt data independently of an identity of the client, the shared key being entered by a user of the client; delivering

the encrypted data from the client to the server; receiving the encrypted data at the server; decrypting the encrypted data, at the server using the shared key, the shared key being stored in a user private keys database; and processing the decrypted data, when where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data.

44. (Previously) The method of claim 43, wherein processing the decrypted data includes the steps of: encrypting the decrypted data with a private server key; and storing the encrypted data, in a database.

45. (Previously) The method of claim 43, wherein the step of processing the decrypted data includes the steps of: encrypting the data with an other user's private key shared between the other user and the server; and sending the encrypted data to the other user.

46. (Previously) The method of claim 43, wherein the step of processing the decrypted data includes the steps of: decrypting the re-encrypted data with the private server key; encrypting the data with a second user's key shared between the second user and the server; and sending the encrypted data to the second user.

47. (Previously) The method of claim 43, wherein the step of processing the decrypted data includes the steps of: processing the data according to an instruction of the user; re-encrypting the processed data using the user's shared key; and sending the re-encrypted processed data to the user.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance. The present invention is directed to a system for secure transfer of data between a client and a server. Each independent claim identifies the uniquely distinct feature "of an encrypt/decrypt engine using a key shared between the client and server where the shared key is derived from the user's authentication data and the derived shared key is used for encrypting all data". The prior art, Laursen et al (US 6,065,120) discloses a conventional security system between a client and server, either singularly or in combination, fails to anticipate or render the claimed limitation obvious.

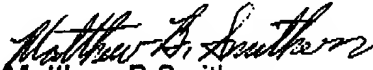
Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew T Caldwell can be reached on (703) 306-3036. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Matthew B Smithers
Primary Examiner
Art Unit 2137